

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/896,242 | 06/29/2001 | Scott Alan Leerssen | 10013503-1 | 9150 |

7590 06/29/2004

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

ANYA, CHARLES E

ART UNIT PAPER NUMBER

2126

DATE MAILED: 06/29/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/896,242

Applicant(s)

LEERSSEN ET AL.

Examiner

Charles E Anya

Art Unit

2126

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 29 June 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>6/14/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-17 are pending in this application
2. The cross references related to the application cited in the specification must be updated (i.e. update the relevant status, with PTO serial numbers where appropriate, on page 1, lines 17 - 20 and page 10 lines 1 - 5 ; The entire specification should be so revised).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. **Claims 1-3,6-11 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,272,519 B1 to Shearer et al. in view of U.S. Pat. No. 6,658,571 B1 to O'Brien et al.**

5. As to claim 1, Shearer teaches a computer readable medium including instructions executable by a processor-based system, said computer readable medium comprising: code for replacing address information in a system call table with address information associated with a plurality of wrapper functions ("Hooking..." Col. 5 Ln. 34 - 47) and code for defining said plurality of wrapper functions (intercept functions 420/425/430) and said plurality of wrappers

Art Unit: 2126

functions transferring processing control to system call routines ("...calling..." Col. 5 Ln. 34 – 47).

6. Shearer is silent with respect to the plurality of wrapper functions retrieving parameters associated with said system call routines, said plurality of wrapper functions utilizing said parameters to generate audit data, and said plurality of wrapper functions writing said audit data to a buffer.

7. O'Brien teaches the plurality of wrapper functions retrieving parameters associated with said system call routines, said plurality of wrapper functions utilizing said parameters to generate audit data, and said plurality of wrapper functions writing said audit data to a buffer (Col. 5 Ln. 56 – 67, Col. 6 Ln. 1 – 4, Col. 8 Ln. 1 - 6).

8. It would have been obvious to one of ordinary skill the art at the time the invention was made to combine the teachings of O'Brien and Shearer because the teaching of O'Brien would improve the system of Shearer by providing means for replaying system calls (Col. 8 Ln. 1 – 6).

9. As to claim 2, Shearer teaches the computer readable medium of claim 1 further comprising: code for copying said system call table to a new memory location as an original system call table copy before replacing said system call table with address information associated with said plurality of wrapper functions (Col. 5 Ln. 50 – 64, Col. 7 Ln. 30 – 42).

Art Unit: 2126

10. As to claim 3, Shearer teaches the computer readable medium of claim 2 wherein at least one of said plurality of wrapper functions is operable to examine memory information of said original system call table copy (Col. 8 Ln. 35 – 47) and is operable to transfer control to a system call routine associated with said memory information (figure 4 Col. 5 Ln. 34 – 47).

11. As claim 6, Shearer teaches a method for generating audit data comprising the steps of: placing a wrapper function in memory/writing address information into an entry of a system call table (“Hooking...” Col. 5 Ln. 34 – 47), said address information being associated with said wrapper function (“...pointer...” Col. 5 Ln. 34 – 47) and transferring processing control to said wrapper function, said wrapper function transferring processing control to a system call routine (“...calling...” Col. 5 Ln. 34 – 47).

12. Shearer is silent with respect to retrieving parameters associated with said system call routine, utilizing said parameters to generate audit data, and writing said audit data to a buffer.

13. O'Brien teaches retrieving parameters associated with said system call routine, utilizing said parameters to generate audit data, and writing said audit data to a buffer (Col. 5 Ln. 56 – 67, Col. 6 Ln. 1 – 4, Col. 8 Ln. 1 - 6).

14. It would have been obvious to one of ordinary skill the art at the time the invention was made to combine the teachings of O'Brien and Shearer because the teaching of O'Brien would improve the system of Shearer by providing means for replaying system calls (Col. 8 Ln. 1 – 6).

15. As to claim 7, Shearer teaches the method of claim 6 wherein said entry is associated with a vector, said method further comprising the step of: generating a system call utilizing said vector (Col. 5 Ln. 50 – 62).

16. As to claim 8, Shearer teaches the method of claim 6 further comprising the steps of: copying an original entry in said system call table associated with said vector to a new location (Col. 5 Ln. 50 – 62).

17. As to claim 9, Shearer teaches the method of claim 8 further comprising the steps of: accessing said copy of an original entry to obtain memory information related to said system call routine (Col. 7 Ln. 30 – 42) and transferring processing control to said system call routine (Col. 8 Ln. 24 – 32).

18. As to claim 10, Although Shearer does not explicitly teach the method of claim 6 wherein said step of transferring processing control includes generating a software interrupt, it is inherent that during each request for processor time (which happens during process control transfers) interrupts are initiated.

19. As to claim 11, Shearer teaches the method of claim 6 further comprising the step of: disabling said wrapper function by restoring original address information to said entry of said system call table (Col. 9 Ln. 29 – 32).

Art Unit: 2126

20. As to claim 14, Shearer teaches a computer system for generating audit data associated with system calls, said computer system comprising: means for receiving processing control, said means for receiving being operable to transfer processing control to a system call routine (Col. 8 Ln. 24 – 32) and means for transferring control to said means for receiving, wherein said means for transferring control includes a system call table with address information associated with said means for receiving processing control (Col. 5 Ln. 34 – 47).

21. Shearer is silent with respect to being operable to generate audit data associated with said system call routine.

22. O'Brien teaches the step of being operable to generate audit data associated with said system call routine (Col. 5 Ln. 56 – 67, Col. 6 Ln. 1 – 4, Col. 8 Ln. 1 - 6).

23. It would have been obvious to one of ordinary skill the art at the time the invention was made to combine the teachings of O'Brien and Shearer because the teaching of O'Brien would improve the system of Shearer by providing means for replaying system calls (Col. 8 Ln. 1 – 6).

24. As to claim 15. The computer system of claim 14 further comprising: means for creating a copy of an original system call table (Col. 5 Ln. 50 – 67), and wherein said means for receiving processing control is operable to determine the memory location of said kernel system call routine by accessing said copy of said original system call table (Col. 7 Ln. 30 – 42).

Art Unit: 2126

25. As to claim 16, O'Brien teaches the computer system of claim 14 wherein said means for receiving processing control includes means for writing audit data to an audit buffer (Col. 7 Ln. 64 – 67).

26. Claims 4,13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,272,519 B1 to Shearer et al. in view of U.S. Pat. No. 6,658,571 B1 to O'Brien et al. as applied to claim 1 above, and further in view of U.S. Pat. No. 6,711,572 B2 to Zakharov et al.

27. As to claim 4, Shearer teaches to the computer readable medium of claim 1 further comprising: code for examining an amount of audit data in said buffer.

28. Shearer as modified by O'Brien is silent with respect code for writing said audit data to an audit file when the amount of audit data in said buffer exceeds a predetermined amount.

29. Although Zakharov does not explicitly teach writing said audit data to an audit file when the amount of audit data in said buffer exceeds a predetermined amount, he does indicate that collected/audit data would transferred at an "appropriate time" which to one of ordinary skill in the art could include when the spool directory/buffer is filled to some level (Col. 5 Ln. 1 – 9, Ln. 36 – 48).

30. It would have been obvious to one of ordinary skill in the art at the time the invention to combine the teachings of Zakharov, Shearer and O'Brien because the teaching of Zakharov would improve the system of Shearer as modified by O'Brien by preventing

31. As to claims 13 and 17, see the rejection of claim 4.

32. Claims 5 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,272,519 B1 to Shearer et al. in view of U.S. Pat. No. 6,658,571 B1 to O'Brien et al. as applied to claim 1 above, and further in view of U.S. Pat. No. 6,728,840 B1 to Shatil et al.

33. As to claim 5, Shearer as modified by O'Brien is silent with respect to the computer readable medium of claim 1 wherein at least one of said plurality of wrapper functions comprises code for performing a logical comparison of said parameters against predefined criteria to determine whether to write audit data to said buffer.

34. Shatil teaches to the computer readable medium of claim 1 wherein at least one of said plurality of wrapper functions comprises code for performing a logical comparison of said parameters against predefined criteria to determine whether to write audit data to said buffer (Col. 13 Ln. 1 – 48).

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Shatil, O'Brien and Shearer because the teaching of Shatil would improve the system of O'Brien and Shearer by providing instructions for caching data (Col. 13 Ln. 10 – 18).

36. As to claim 12, see the rejection of claim 5.

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Pat. No. 6,282,703 B1 to Meth et al. discloses a technique for statically inking an application process to a wrapper library used in intercepting calls invoked by application process.

U.S. Pat. No. 6,560,613 B1 to Gylfason et al. discloses a method for intercepting system calls via a wrapper and determining whether the validity of the desired file type.

38. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Charles E Anya whose telephone number is (703) 305-3411. The examiner can normally be reached on M-F (8:30-6:00) First Friday off.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, An Meng-Ai can be reached on (703) 305-9678. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2126

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Charles E Anya
Examiner
Art Unit 2126

cea.


MENG-AL T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100